

Weekly Report

2016.04.18-2016.04.24

1.This Week

Graduation Design

Working on the coding part of my graduation design and preparing to start writing paper next week.

Survey

Classify all the documents and use [coding.net](#) to manage them. Each single paper is uploaded with a brief conclusion and updated every time it is reviewed.

The image shows a screenshot of a file management interface (likely a web-based file explorer) and a PDF document titled "PortVis.pdf".

File Management Interface:

- Top bar: Search, 项目, 任务, IDE, 偏好, 升级, 帮助. This-is-a-lovely-survey.
- Left sidebar: 项目文件, 分享中, 默认文件夹, General_Methods, Traffic_data_Vis, HistoryLog, Cyber_Trust, Other_Survey, Cyber_Attack_Dete..., Situational_Aware..., Network_generally.
- Main area: 默认文件夹. 还来上传任何文件, 点击或将文件拖拽至此页面上方! 支持所有文件格式, 单个文件不超过100M.

PortVis.pdf Document:

PortVis: A Tool for Port-Based Detection of Security Events

Jonathan McPherson, Kwan-Liu Ma
University of California at Davis

Paul Krystosk, Tony Bartoletti, Marvin Christensen
Lawrence Livermore National Laboratory

ABSTRACT

Most visualizations of security-related network data require huge amounts of finely detailed, high-dimensional data. However, in some cases, the data available can only be coarsely detailed because of security concerns or other limitations. How can interesting security events still be discovered in data that lacks important details, such as IP addresses, network security alarms, and labels? In this paper, we discuss a system we have designed that takes very coarsely detailed data—basic, summarized information of the activity on each TCP port during each given hour—and uses visualization to help uncover interesting security events.

Categories and Subject Descriptors

C.2.0 [Computer-Communication Networks]: General—Security and Protection; H.3.1 [Information Storage and Retrieval]: Content Analysis and Indexing—Abstracting methods; H.5.2 [Information Interfaces and Presentation]: User Interfaces; I.3.8 [Computer Graphics]: Applications

General Terms

Algorithms, design, security, human factors.

Keywords

Network security, information visualization, user interfaces

recorded in security logs, but these logs are time-consuming for administrators to try to analyze by hand. Therefore, many attempts have been made to ease the detection of interesting information in the logs, using both traditional information visualization mechanisms like parallel coordinates, self-organizing maps, and multi-dimensional scaling, and novel visualization mechanisms designed specifically for this task [3, 5].

Unfortunately, the level of attacks on a network is likely to be directly proportional to the value of the network. Networks that contain company or government secrets are more likely to be targeted by criminals inside or outside the network; large, high-profile networks make tempting targets for Internet terrorists. Therefore, network administrators can find themselves in a quandary when it comes to seeking outside network security help. They may not be permitted to reveal very much information about their networks' internal structure to security analysts, yet the analysts need a great deal of this information to do their jobs, since security visualization tools are likely to require very detailed data. For example, the SUM network security visualization system [4] requires information about each individual packet that goes across the network! Not all visualization systems require this level of detail, but most require, at the very least, IP address information.

Since information about the network's size, structure, and other important attributes may be sensitive, it is expedient to look at visualizations that permit network security events

History:

- leestrong 上传了新版本 V1 PortVis.pdf 04-21 19:47
- leestrong Portvis是基于散点图设计的, 它使用了3种不同的视图可视化展示TCP流量, 分别是时间线可视化, 主视图和端口可视化, 时间线视图有选择器可以选择时间段, 主视图是一个256*256的散点图, 每个点代表一个端口, 以颜色代表端口数值, 定义了一个选择器可以选定区域方大角提供其信息, 端口可视化中以3D的形式表现端口的信息, 但是时间数据定义的非常粗糙使得按时间找pattern很困难, 另外端口网格填满颜色可能会使一些极端的端口信息过载。
- poopcorn 移动了文件 PortVis.pdf 04-22 16:45

按此键输入评论内容 (Command+Enter)

2.To Do

- (1) Continue working on my graduation design.
- (2) Finish the outline of this survey and prepare for writing.